February 16, 2023

Washington My Health My Data Act (HB 1155)

Comments from the Software & Information Industry Association (SIIA)

The Software & Information Industry Association (SIIA) writes to provide recommendations on Washington's My Health My Data Act legislation (H.B. 1155). We appreciate the special consideration of health data privacy legislation this session. We propose amendments to devise a meaningful industry standard that protects consumer rights and strengthens data privacy safeguards.

SIIA is the principal trade association for the software information and digital content industry representing more than 450 information and technology companies, including the global industry leaders for the digital age: software, data analytics, and information service companies.

SIIA supports privacy as a fundamental value, one essential to individual autonomy and a functioning democracy. We have shared feedback similar to the below that has been accepted by a significant number of states that advanced consumer privacy legislation, laws, and respective regulations.

Recommendation 1: Refine the definition of "consumer health data"

The bill's definition of consumer health data is overbroad and would sweep in a wide range of personal data that may not be used in a health specific context or may not relate to the health data privacy interests the legislation seeks to protect. Overbreadth in this area would specifically increase confusion and interruptions of everyday tasks for consumers, while creating complicated compliance challenges for Washington businesses.

A recent article "Data is What Data Does: Regulating Use, Harm and Risk, Instead of Sensitive Data," by the renowned privacy scholar and GWU law professor Daniel Solove, addresses the tradeoff between regulating risk with regulating data[1]. Professor Solove notes that it is not meaningful to try and accurately regulate inferences, as almost all personal data – and in some cases, data that is publicly available and subject to First Amendment protections – may get swallowed into the sensitive data category, which creates unnecessary overbreadth. He states: "The particular type of personal data does not indicate anything important when it comes to determining how to protect it. What matters is use." The legislation will likely lose its impact and be so wide in scope that it no longer protects consumers interests, if it does not narrow the definitions further, and avoid regulating inference, proxy, and other types of data.

[1] Solove, Daniel J., Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data (January 11, 2023). Available at SSRN: https://ssrn.com/abstract=4322198 or http://dx.doi.org/10.2139/ssrn.4322198

We recommend the following revisions:

(8)(a) "Consumer health data" means personal information that is linked or reasonably linkable to an identified or identifiable consumer and that the Regulated Entity processes for the purpose of revealing the consumer's past, present, or future physical or mental health diagnosis or access to health care services. Consumer health data may include, but is not limited to:

(i) Individual health ~~conditions~~, treatment, status, diseases, or diagnoses;

(ii) Medical interventions, including Social, psychological, and behavioral~~, and medical~~ interventions;

(iii) Health-related surgeries or procedures;

(iv) Use or purchase of medication

(v) ~~Bodily functions,~~ V~~v~~ital signs, symptoms, or measurements of

(vi) Diagnoses or diagnostic testing, treatment, or medication;

(vii) Gender-affirming care information;

(viii) Reproductive or sexual health information;

(ix) Biometric data related to information described in this subsection (8) (a);

(x) Genetic data related to information described in this subsection (8) (a);

~~(xi) Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies; or~~

~~(xii) Any information described in (a)(i) through (xi) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivate, inferred, or emergent data by any means, including algorithms or machine learning).~~

(b) "Consumer health data" does not include:

(i) personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the Regulated Entity, the expected benefits of the research outweigh the privacy risks, and if the Regulated Entity has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; ~~that the regulated entity has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.~~

(ii) Personal information that is not processed for the purpose of revealing the consumer's past, present, or future physical or mental health diagnosis or access to health care services.

Recommendation 2: Remove the private right of action (Section 11).

Section 11 of the bill would create a private right of action (PRA), where consumers can bring lawsuits against covered entities for violations of the bill. The broad definition of "consumer health data" makes the inclusion of a PRA especially problematic, because it brings non-health data into scope, and thus could lead to a much broader range of potential violations. The effect of including a PRA will be staggering litigation costs for technical violations, without limit. We are concerned that our members will be subjected to frivolous lawsuits based on technical violations where there is no actual harm or injury done. This will lead to increased costs for consumers as companies will be forced to settle meritless claims or engage in expensive litigation to defend against technical violations of the statute.

Moreover, inclusion of a PRA in the bill will neither provide meaningful consumer privacy protections nor advance business compliance safeguards. Such a provision has also never been enacted in any state consumer privacy law to date. Rather, a PRA will chill beneficial data use and increase the costs to the consumers as controllers desperately try to insulate themselves against this kind of risk.

On the other hand, Attorney General enforcement, which will by its nature involve the exercise of discretion, would be a much more effective mechanism for addressing those instances in which individuals have been harmed by violations of the statute. Thus, we recommend striking Section 11, and instead, including reference to enforcement solely by the Attorney General.

We recommend the following revisions:

Sec. 11. ~~The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business, and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.~~

(1) This chapter may be enforced solely by the attorney general under the consumer protection act, chapter 19.86 RCW 7.
(2) The legislative declarations in this section do not apply to any claim or action by any party other than the attorney general alleging that conduct regulated by this chapter violates chapter 1819.86 RCW, and this chapter does not incorporate RCW 19.86.093.19.
(3) Nothing in this Chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this Chapter or any other law.
(4) The Attorney General shall, prior to initiating any action for a violation of any provisions of this Chapter, issue a notice of violation to the Regulated Entity or processor if the Attorney General determines that a cure is possible. If the Regulated Entity or processor fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section.

Recommendation 3: Refine the definition of "regulated entity."

As written, the bill's provisions are overly broad and would therefore covers entities that have little or nothing to do with health care. To limit this overbreadth, we recommend revising the definition of "Regulated Entities" by inserting reference to "entities that market themselves as providing care for or diagnosis and consultation of health services" as a necessary requirement to be considered a legal entity subject to this bill. This revised definition will serve to further clarify the bill's scope, and ensure it is targeted in applying heightened protections for health data as intended.

We recommend the following revisions to Section 3 (23):

(23) "Regulated entity" means any legal entity that: (a) Conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; ~~and~~ (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data; and (c) markets itself as primarily providing care for or facilitating the diagnosis, consultation, treatment, education, care management, or self-management of physical or mental health care services. "Regulated entity" does not mean government agencies, tribal nations, or contracted service providers when processing consumer health data on behalf of a government agency.

Recommendation 4: Revise the Definition of "Biometric Data" (Section 1).

In Section 3, we recommend that the bill refine its definition of biometric data. As written, the bill defines "Biometric Data" to include "data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data." This definition varies from the more precise definition of biometric identifier that exists in Washington's Biometric Privacy Protection Act[2]. To avoid conflicting interpretations of this legislation with the existing biometrics law in Washington, we recommend using the existing biometrics identifier definition. Doing so will create uniformity and streamline the interpretation of the law for business compliance.

We recommend the following revisions:

Strike the following from Section 3 (4):

~~(4) "Biometric data" means data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data. Biometric data includes, but is not limited to:~~

~~(a) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or~~

~~(b) Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information.~~

[2] Washington Chapter 19.375, Enacting HB 1493. https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true

Replace with the following new definitions:

(1) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

Recommendation 5: Revise the Definition of "Reproductive and Sexual Health Information" (Section 3).

As noted earlier, the type of data is not as important as the use of the data; otherwise we are likely to see a chilling effect on research and development and the innovation ecosystem more broadly. Rather than regulating all inferences and extrapolations tied to reproductive or sexual health information, it would be more effective to regulate reproductive or sexual health information as it relates to geolocation data that could reasonably indicate a person is attempting to acquire reproductive or sexual health services.

We recommend the following revisions to Section 3 (24):

(24) "Reproductive or sexual health information" means personal information relating to seeking or obtaining past, present, or future reproductive or sexual health services. "Reproductive or sexual health information" includes, but is not limited to~~: (a)~~ precise location information that could reasonably indicate a consumer's attempt to acquire or receive reproductive or sexual health services.

~~(a) Efforts to research or obtain reproductive or sexual health services; or~~

~~(b) Any reproductive or sexual health information that is derived, extrapolated, or inferred, including from nonhealth information (such as proxy, derivative, inferred, emergent, or algorithmic data).~~

Recommendation 6: Revise the Definition of "Collect" (Section 3).

As noted previously, the definition of collect goes well beyond reasonable understandings of collection or acquiring data to also include other processing such as mere transmission of data. In addition, inferences and derivatives are not a form of collection, but a creation by the entity. We do not believe this is the intent and ask that the definition remove language that would capture much broader activity and sweep in routine uses of non health data for consumers.

We recommend the following revisions to Section 3 (5):

(5) "Collect" means to buy, rent, access, retain, receive, or acquire~~, infer, derive, or otherwise process~~ consumer health data in any manner.

Recommendation 7: Add common sense operational exemptions (Section 12).

Consumer privacy laws passed in the last few years have agreed on a number of exemptions and limitations, recognizing legitimate business uses for defending against legal claims, responding to valid law enforcement requests, conducting internal research to improve or repair products, services or technology, or perform internal operations that are reasonably aligned with the expectations of the consumer. We urge these provisions from other state consumer privacy laws[3] be added into the bill.

Recommendation 8: Remove overly restrictive terms around sharing and deletion.

The privacy laws in other states have not added additional restrictive terms to the handling of data, even sensitive data. The insertion of terms like "to the extent necessary" rather than "reasonably necessary" or the requirement that companies inform every affiliate, third party and processor of deletion requests are not present in the other privacy laws. These create unique burdens on Washington companies and national companies seeking to serve Washingtonians. We urge you to make the bill interoperable with the other state consumer privacy laws, rather than create these discrepancies.

We recommend the following revisions to Section 5:

(1) A regulated entity may not collect any consumer health data except:
(a) With consent from the consumer for such collection for a specified purpose; or (b) ~~To the extent~~ As reasonably necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity.
(2) A regulated entity may not share any consumer health data except:
(a) With consent from the consumer for such sharing that is separate and distinct from the consent obtained to collect consumer health data; or
(b) ~~To the extent~~ As reasonably necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity.

Conclusion

We believe these recommendations are beneficial to industry and consumers alike. We urge the legislature to review the changes and apply them, prior to any further movement on the bill this legislative session. SIIA supports privacy as a fundamental value, one essential to individual autonomy and a functioning democracy. We believe that an interoperable state data privacy standard that harmonizes meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of uniform data privacy practices.

We appreciate your willingness to consider these recommendations in regards to this bill, as we believe the changes will create consistent, comprehensive consumer privacy safeguards. If you have further questions, please contact Divya Sridhar, at dsridhar@siia.net.

Sincerely,

[3] See: Virginia Consumer Data Protection Act § 59.1-582. (Effective January 1, 2023) Limitations.

Divya Sridhar, Ph.D.

Senior Director, Data Policy

Software & Information Industry Association